

## UNITED STATES DISTRICT COURT

WESTERN

for the  
DISTRICT OF

OKLAHOMA

FILED  
APR 28 2022MELITA REEDER SHINN, CLERK  
U.S. DIST. COURT - WESTERN DIST. OK  
BY

In the Matter of the Search of )

A black in color Apple iPhone 11, )  
bearing IMEI No. 350320525646129, and )  
a black in color Samsung cellular smart phone, )  
bearing IMEI No. 359265100989223 )

Case No: M- 22-311-SM

## APPLICATION FOR SEARCH WARRANT

I, Scott Muncaster, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

Title 18, U.S.C., § 1470  
Title 18, U.S.C., § 2251

Attempted transfer of obscene material to a minor  
Attempted sexual exploitation of a child

The application is based on these facts:

See attached Affidavit of Special Agent Scott Muncaster, HSI, which is incorporated by reference.

☒ Continued on the attached sheet(s).  
☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



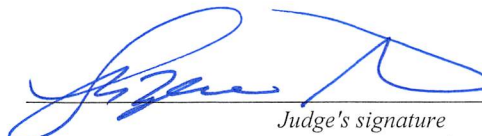
*Applicant's signature*

Scott Muncaster, Special Agent  
HSI

Sworn to before me and signed in my presence.

Date: April 28, 2022

City and State: Oklahoma City, Oklahoma



*Judge's signature*

SUZANNE MITCHELL, U.S. Magistrate Judge

*Printed name and title*

**THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF OKLAHOMA**

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Scott Muncaster, a Special Agent with the Department of Homeland Security, Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”) since May 2017, and I am currently assigned to the office of the Resident Agent in Charge, Oklahoma City. I am also an investigative member of the Oklahoma Internet Crimes Against Children (OK ICAC) taskforce. While employed by HSI, I have been involved in investigations of child exploitation matters and computer crimes against children. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as a Special Agent with HSI.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Dylan LILES, who is alleged to have attempted to transfer obscene material to a minor, in violation of 18 U.S.C. § 1470, and attempted to sexually exploit a child, in violation of 18 U.S.C. § 2251(a) and (e), collectively referred to as the “SUBJECT OFFENSES.”

4. This Affidavit seeks authorization to search (i) a Black Apple iPhone 11 and

(ii) a Black Samsung phone, further described in Attachment A and collectively referred to as the “SUBJECT DEVICES,” and seize therefrom the items described in Attachment B, which constitute instrumentalities, fruits, and evidence of the SUBJECT OFFENSES.

5. HSI Special Agents seized the SUBJECT DEVICES from LILES’S residence, located at 1109 N. 11<sup>th</sup> Street, Duncan, Oklahoma 73522 (the “SUBJECT PREMISES”), on April 21, 2022, during the execution of a federal search warrant related to the investigation into LILES. The SUBJECT DEVICES are currently secured at the HSI Oklahoma City Field Office, located at 3625 NW 56<sup>th</sup> St., Oklahoma City, Oklahoma 73112. As set forth below, there is probable cause to believe that LILES possessed, owned, and used the SUBJECT DEVICES to commit the SUBJECT OFFENSES.

6. The facts in this Affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

7. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

8. I know that cellular telephones are often equipped with digital cameras and

those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

9. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications, as well as applications like Snapchat. Additionally, individuals utilize their cellular devices to take and store pictures and keep notes. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual.

10. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during, and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text

messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information.

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the SUBJECT OFFENSES, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques (including but not limited to computer-assisted scans of the entire medium) that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

13. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, there is reasonable cause to authorize execution of the warrant at any time in the day or night.

14. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the SUBJECT DEVICES. This method is analogous to cursorily

inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

### **BACKGROUND ON KIK MESSENGER**

15. As explained below, there is probable cause to believe that LILES committed the SUBJECT OFFENSES, in part, through the use of Kik Messenger—a free service easily downloaded from the Internet. Kik advertises itself as “the first smartphone messenger with a built-in browser.” According to the company’s website, Kik Messenger has become the simplest, fastest, most life-like chat experience one can use on a smartphone. Unlike other messenger apps, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.



16. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google Play Store for Android devices. Kik can be used on multiple mobile devices, including cellular phones and tablets.

17. In general, Kik asks each of its subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, this information is not verified by Kik.

18. Kik typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. Kik often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. In addition, generally Kik maintains at least the last 30 days of all communications for each Kik user.

19. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to



obtain a different username. In addition to a username, a Kik user may display a traditional name within the app, hereinafter referenced as the user's "handle."

20. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e., a phone number), Kik has become a popular app used by people involved in the collection, receipt, and distribution of child pornography

### **STATEMENT OF PROBABLE CAUSE**

21. On or about December 6, 2021, LILES, using Kik, with the username "firefighter9208" and handle "Dylan Adams," initiated a chat dialogue with an HSI Special Agent, acting in an Undercover (UCA) capacity as a 13-year-old girl from New Jersey on Kik. The following is a summary of the conversation between the UCA and LILES, utilizing the Kik social messaging application and SMS text messaging from December 6, 2021, to March 30, 2022:

a. On December 6, 2021, the UCA received an unsolicited message from firefighter9208—to which I have probable cause to believe is LILES'S Kik username, as explained below—stating, "Hey what's up." After the UCA responded to LILES, LILES told the UCA that he had been a firefighter for 12 years, starting in Kansas and now in Oklahoma. After additional back-and-forth, LILES told the UCA that he was 28 years old, to which the UCA replied that she was too young for him and did not want to get into trouble. LILES next asked the UCA how old she was, and the UCA stated that LILES could get into trouble. LILES continued to press the issue, promising not to report the UCA. The UCA then told LILES that she was 13 years old. After additional conversation, LILES

asked the UCA to “come be [his] company.”

b. The UCA and LILES continued to chat over the subsequent days. On December 28, 2021, LILES asked the UCA for a picture. The UCA provided a picture of herself standing in a bathroom in a black shirt. Upon receiving the photograph, LILES told the UCA that he was “kinda horny,” and asked the UCA, “[w]anna help me” and “what naughty things have you done?” As to the latter question, the UCA responded, “not much im only 13 remember lol.” LILES proceeded to ask the UCA a series of sexually charged questions, including, “you ever touched a guy,” “been touched,” and “where was the touching at?” LILES then asked the UCA for additional pictures, promising to not “blast anything” and that he would “just enjoy it,” adding a winking emoji to the latter message.

c. After additional back-and-forth, LILES messaged the UCA, “I’d touch you right. You would love it. Especially when I use my tongue on your vagina.” LILES also told the UCA, “I’m touching myself to your picture,” and proceeded to send the UCA a photograph of an erect penis, alongside the message, “Do you have any cute friends with kik?” Thereafter, LILES asked the UCA if she received his picture and noted, “That was because of your picture.” LILES then asked the UCA for a picture of her boobs, to which the UCA responded, “I don’t want to.” Later, the UCA sent LILES a picture purporting to be of herself. The picture depicted the UCA in the bathroom wearing a tank top. LILES responded, “I can’t see anything.”

d. On December 29, 2021, at approximately 10:48 AM EST, LILES messaged the UCA, “Good morning gorgeous!” In reference to LILES’S Kik handle, the

UCA asked LILES if Dylan is his real name, to which LILES responded, “Yes it is.” After additional back-and-forth regarding LILES’S pet dogs, LILES told the UCA to “come play.” The UCA then asked LILES if they could text instead of using the Kik app and sent LILES her phone number.

e. On the same day, at approximately 11:36 AM EST, the UCA received a text from phone number 580-725-7419, stating “Hello gorgeous.” As explained in more detail below, based on information from that number’s cellular service provider, I have probable cause to believe the number was used by LILES during the relevant period. The conversation continued over the next several days. On December 31, 2021, LILES asked the UCA, “Can I see you?” On January 1, 2022, LILES messaged the UCA, “Come hang out with me.” In reference to New Year’s Eve, LILES also asked the UCA, “Did you get a kiss at midnight,” and “[h]ow about we kiss lol.” On January 5, 2022, LILES asked the UCA for a picture, to which the UCA sent him a picture purporting to be of herself in a black top. Upon receiving the picture, LILES responded, “Come over lol.”

f. The UCA did not again communicate with LILES for nearly a month. On February 2, 2022, LILES messaged the UCA via Kik, stating that his phone broke and he had lost his contacts. The UCA responded on February 14, 2022, with “hey.”

g. On February 17, 2022, at approximately 2:23 PM EST, LILES messaged the UCA via Kik, asking, “What’s up” and “[c]an I see you?” After additional back-and-forth, the UCA asked for a picture of LILES, to which LILES responded, “Let me see you first lol.” The UCA next sent a picture purporting to be of herself in a bathroom wearing a

tank top, to which LILES responded, “I’d love to see more of you.” LILES also responded with a picture of himself with no shirt on. LILES also asked the UCA, “Can I see your body?”

h. On February 28, 2022, the UCA sent LILES a Kik message “hey.” The UCA received a message stating LILES’S phone has been off/disconnected for a while and the message would be delivered when LILES connects again.

i. On March 23, 2022, the UCA reinitiated contact with LILES via Kik. On March 30, 2022, at approximately 3:45PM EST, LILES sent the UCA a photograph of an erect penis, alongside the messages, “I’m horny” and “can I see you?” After additional back-and-forth, the UCA told LILES that she was walking around with her mother because she was too young to stay home alone. The UCA noted that she could stay home alone once she turned “14,” to which LILES responded, “Well damn 14 needs to hurry up.”

j. That same day, LILES asked the UCA, “you want to come shower with me?” LILES proceeded to describe in detail what he would do to the UCA were they alone together: “How about I pick you up and grasp your butt while you wrap your legs around me and carry you to the room;” “[t]hen I gently lay you down on the bed and slowly kiss your lips, down your neck, chest, stomach;” “slowly kissing your inner thighs and slowly moving closer to your vagina;” “[w]hile kissing your vagina my tongue will gently go across your clit, my hand will be on your boob, your back will start to bow;” “I’ll slowly enter one finger inside you as I keep using my mouth;” “[t]hen I’ll kiss my way back up your body and slowly enter my dick inside you;” and “[t]hen right before I get off I’ll pull

out and cum all over you.” The UCA last made contact with LILES on April 19, 2022.

22. The UCA conducted a search of phone number 580-725-7419 within a commercially available public records database. The search revealed that phone number 580-725-7419 was assigned to subscriber, Onvoy, LLC.

23. On or about January 3, 2022, an HSI summons was issued to Onvoy, LLC, requesting information regarding cellular telephone number 580-725-7419.

24. On or about January 27, 2022, from the summons results, it was determined that telephone number 580-725-7419 is assigned to service provider TextNow, Inc.

25. On or about January 31, 2022, an HSI summons was issued to TextNow, Inc., requesting information regarding telephone number 580-725-7419.

26. On or about January 31, 2022, from the summons results, it was determined that telephone number 580-725-7419 was assigned to an account with username dylanliles08, an associated email address dylanliles08@gmail.com, and the Registration Internal Protocol (IP) 160.3.191.198. The information received from TextNow also revealed an active use date for the number from December 29, 2021, to January 29, 2022.

27. On March 9, 2022, I used commercially available software to determine that the IP address 160.3.191.198 is registered to the Internet Service Provider Cable One Inc. a/k/a/ Sparklight. Results received from Sparklight, in response to a summons dated March 10, 2022, revealed that the IP address is assigned to Chloe Gamblin at the SUBJECT PREMISES. According to Sparklight records, Chloe Gamblin’s account is active, and she has been a customer since September 28, 2020.

28. Open-source research revealed LILES is a resident of the SUBJECT PREMISES. I also determined that LILES is married to Chloe Gamblin.

29. On Friday, March 18, 2022, I traveled to Duncan, Oklahoma, to conduct visual surveillance of the SUBJECT PREMISES. In doing so, I observed a white Dodge Ram pickup truck (with License Number OK #KOZ-811) parked in front of the residence. Records indicate that the Ram in question is registered to Dylan Liles.

30. On March 25, 2022, a summons was sent to Media Lab-KIK for Kik username “firefighter9208.” Information received from Media Lab-KIK revealed that username firefighter9208 is registered to “Dylan Adams” with an associated email of dylanliles07@gmail.com.

31. I also ran an Accurint Virtual Identity Report on LILES. The Report listed LILES’S address as that of the SUBJECT PREMISES. In addition, the report listed dylanliles07@gmail.com as an associated email account.

32. On April 8, 2022, I applied for and received a federal search warrant for LILES’S residence from Magistrate Judge Amanda Green. The search warrant was executed on April 21, 2022.

33. Upon execution of the search warrant on, LILES, Chloe Gamblin, and their four minor children were encountered at the SUBJECT PREMISES by Duncan Police Department Special Response Team personnel. During a pat-down search by officers of LILES’S person, a black Apple iPhone—one of the SUBJECT DEVICES—was found inside a pocket of LILES’S gym shorts.

34. Additionally, while searching the SUBJECT PREMISES, HIS Special Agents discovered a black Samsung cellular smart phone—one of the SUBJECT DEVICES—on a cabinet in the front family room. On her own volition, Chloe Gamblin told HSI Agents that she believed the Samsung phone belonged to LILES.

35. During the search of LILES'S bedroom, agents found a bright blue fleece blanket on LILES'S bed matching the image of a blanket in the background of the explicit photographs LILES sent the UCA. The agents also observed a flat screen television mounted over a short television stand that match a corresponding television and stand in the background of the explicit photographs.

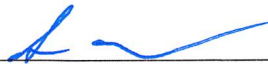
36. During an audio/video recorded, consensual interview of LILES during the search, LILES confirmed that the aforementioned black Apple iPhone belonged to him. LILES provided HSI Special Agents with a numeric passcode to unlock the Apple iPhone and verbal consent to preview the contents of the Apple iPhone. LILES stated that he did not know the passcode to the black Samsung phone.

37. Additionally, during the interview, HSI Agents provided LILES printouts of the Kik chat between Kik account user “firefighter9208” and the UCA. LILES stated that the profile picture associated to the account “firefighter9208” was in fact him and that it was his account. He otherwise denied that he had sent the chats in question to the UCA, however, and claimed he had not used Kik in some time.



**CONCLUSION**

38. Based on the foregoing, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT DEVICES. I respectfully request that this Court issue a search warrant authorizing the search of the SUBJECT DEVICES described in Attachment A to seize the items described in Attachment B. I know digital files can be easily transferred back and forth on devices such as the SUBJECT DEVICES and stored simultaneously on such devices.

  
\_\_\_\_\_  
Scott Muncaster  
Special Agent  
Homeland Security Investigations

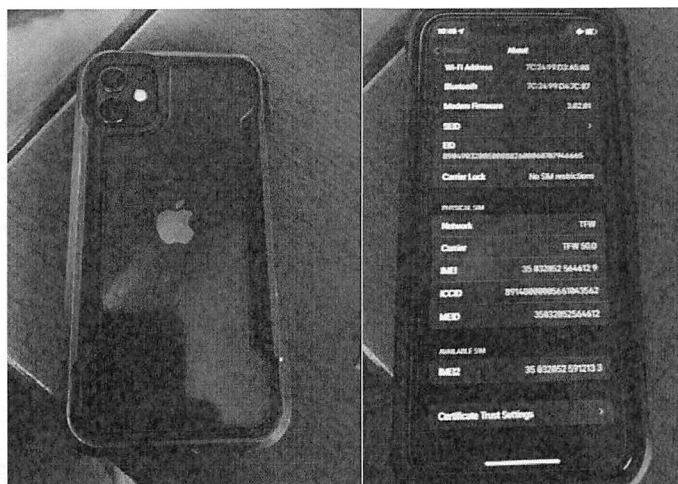
**SUBSCRIBED AND SWORN** to before me this 28 day of April, 2022.

  
\_\_\_\_\_  
SUZANNE MITCHELL  
United States Magistrate Judge

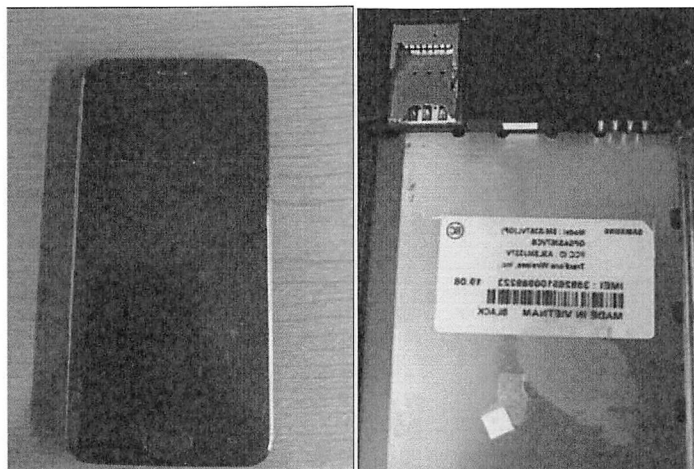
## ATTACHMENT A

### PROPERTY TO BE SEARCHED

This warrant seeks to search: (i) a Black Apple iPhone 11 with red protective case (IMEI #350320525646129), and (ii) a Black Samsung cellular smart phone (IMEI #359265100989223). The SUBJECT DEVICES are currently located at the HSI Oklahoma City Field Office, located at 3625 NW 56<sup>th</sup> Street, Oklahoma City, Oklahoma 73112.



Black Apple iPhone 11 (IMEI #350320525646129)



Black Samsung Cellular Smart Phone (IMEI #359265100989223)

## **ATTACHMENT B**

### **LIST OF ITEMS TO BE SEIZED**

1. All records on the SUBJECT DEVICES described in Attachment A that relate to violations of the SUBJECT OFFENSES:

#### **I. Digital Evidence**

1. Any passwords, password files, test keys, encryption codes, or other information necessary to access the SUBJECT DEVICES;

2. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device described in Attachment A, that show the actual user(s) of the computer or digital device during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the device; MAC IDs and/or Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software; evidence of the absence of such malicious software, or of the presence or absence of security software designed to detect malicious software;

3. Evidence that the device was attached to or used as a data storage device for some other device, or that another device was attached to the device; and

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device;

## **II. Records, Documents, and Visual Depictions**

1. Any records, documents, or materials, including correspondence, that pertain to any conversations with the UCA described in the Affidavit in support of the search warrant application in any form including Kik, or any other social media platform;

2. Any records, documents, or materials, including any correspondence, that involve any communication with any person that appear to be coercive in nature for the purposes of grooming or obtaining images from any person;

3. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

4. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

5. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

6. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

7. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

8. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

9. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet on any app installed on the SUBJECT DEVICES.

10. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received;

11. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or

notes associated with child pornography or those who collect, disseminate, or trade in child pornography; and

12. Any records, documents, materials, videos, or photographs that would allow investigators to ascertain who used the SUBJECT DEVICES;

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.